Internet Broadcasters
Multimedia Server Security Guide

Written By

David Childers

www.ScenicRadio.Com

Relaxing Entertainment for the World

BW

www.BroadcastingWorld.Com

Global Broadcast Information Portal

Creative Common License

This body of work is released under the Attribution-ShareAlike version 3.0, Creative Common License.

The work may be freely distributed or modified for commercial or non commercial purposes.

If this work is modified, compliance with the Attribution-ShareAlike version 3.0, Creative Common License is required.

These requirements include:

- Any derivatives of this work must be attributed to David Childers.
- Alterations, transforming, or building upon this work requires distributing the resulting work only under the same, similar or a compatible license.

For the complete legal code, please refer here:
www.creativecommons.org/licenses/by-sa/3.0/legalcode

Cover graphic - Vanitas Still Life - Public Domain Image.
graphicsfairy.blogspot.com/2011/05/antique-clip-art-skeleton-keys-and-lock.html

Foreword graphic - A Silent Colloquy - Paul Stade, The Magazine of Art, London, 1884.
en.wikipedia.org/wiki/File:Pieter_Claesz_002b.jpg

About The Author

David Childers is the Content Manager for the Global Broadcasting portal www.BroadcastingWorld.com. He is very active in the Internet broadcast industry and has written numerous guides and a book about this growing technological field. He is also the webmaster of www.ScenicRadio.com, the global destination for relaxing entertainment.

Mr. Childers' work has been cited in several national and International publications, including these:

Five Essays on Copyright In the Digital Era
Turre Publishing

Research On High-Profile Digital Video Production
Digital Content Association of Japan

Video Podcasting in Perspective: The History, Technology, Aesthetics and Instructional Uses of a New Medium
Journal of Educational Technology Systems

Video Podcasting: When, Where and How it's Currently used for Instruction
The National Convention of the Association for Educational Communications and Technology

IP Packet Charging Model For Multimedia Services
National University of Rwanda

Preservation of audiovisual mediums: Problems and challenges
Platform for Archiving and Preservation of Art on Electronic and Digital Media

P2P Technology Trend and Application to Home Network
Electronics and Telecommunications Research Institute Journal

Peer To Peer Computing - The Evolution of a Disruptive Technology
Idea Group Publishing

Peer-to-Peer Systems and Applications
Lecture Notes In Computer Science
Springer Berlin / Heidelberg

Feedback

Please feel free to contact the author if you have any questions or comments. Your feedback is greatly appreciated.

You can contact the author here: www.KL7AF.com

Foreword

Greetings,

It is with great joy that I once again delve into the mysterious realms of information. The tide of information grows by vast amounts, and should be considered an important resource that is priceless. Knowledge should be used wisely for the benefit of all and shared with every one.

The musical inspiration for this guide is Chapel Stile from the album Soundcastles by Pretz.

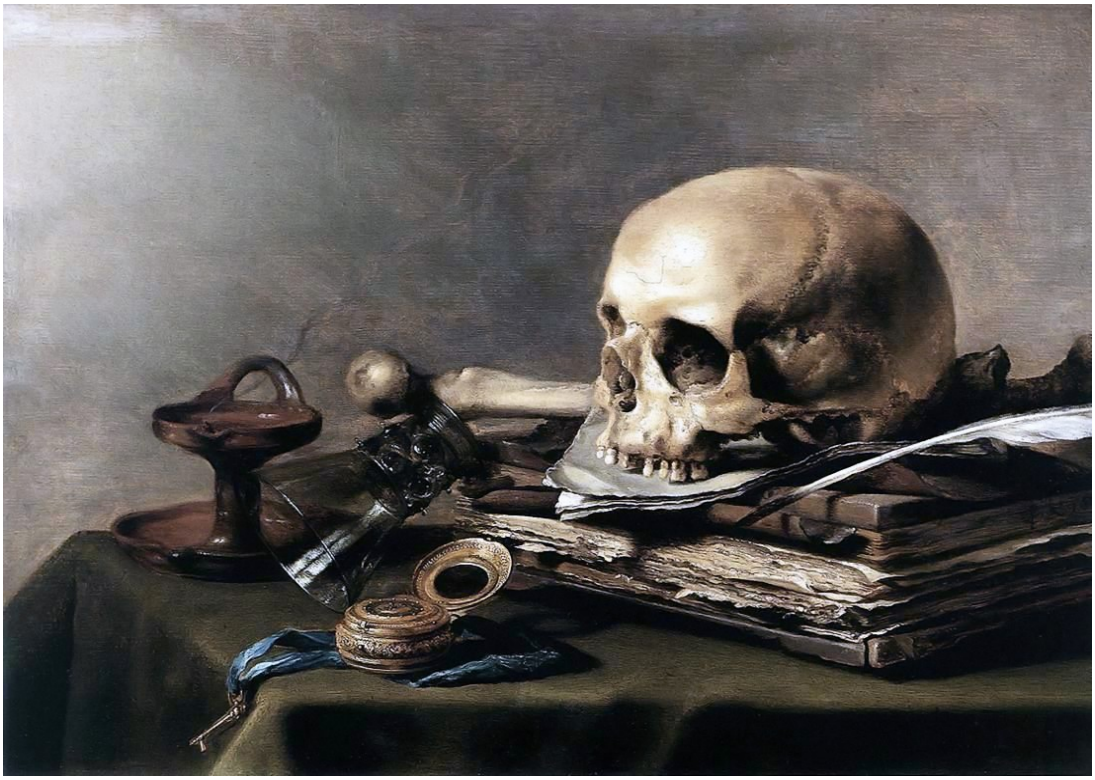
I would like to thank Scarlet Coker for providing assistance with the editing of the manuscript and James Davey at Broadcasting World for allowing me the opportunity to create this guide.

It is my sincere hope that the reader finds this guide beneficial.

David Childers

December 2011

Posveèeno Neži Vidmar.



Ipsa scientia potestas est.

Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts.

William O. Douglas

Index

Introduction

The increase of computer breaches and hacker attacks clearly indicates that computer security is a very important realm of expertise. These threats originate from individuals, cultural, social, and political affiliations as a means to manipulate or create havoc.

System security is not an exact science, but is an ongoing process. Many aspects need to be considered to ensure proper and sustainable security. The mantra of security should be aspired to by every one at the broadcast station. Hackers or computer marauders will not discriminate to achieve their goals, every one is a prime target. Security is only as good as the people implementing it. The lack of enforcement of security standards can allow great damage to occur, regardless of how many manuals or memos are created.

Both the computer system hosting the media server and the actual media server software should be considered equally important for maintaining security. A media server or its computer host that can be compromised or breached by unauthorized persons can financially ruin a broadcaster. This situation can also be exploited to discredit the broadcaster or drive away their audience.

Security starts with the individual; make it a habit to be secure and computer conscious.

Think it. Live it. Do it.

Planning

A detailed plan should be created to outline the methods for maintaining security and initiating recovery from a system failure. Everyone concerned should review the proposed plan prior to finalization and provide input. Once the plan has been finalized, it should be strictly enforced.

This plan should encompass the following:

- Designated personnel for media server administration.
  * Contact information
    - Home telephone number
    - Cell telephone number
    - E mail address

- Contact information for system administration of remotely hosted computers.
  * Trouble desk
    - Telephone number
    - E mail address
  * Help desk
    - Telephone number
    - E mail address

- Contact information for network administration of uplink data feed.
  * Trouble desk
    - Telephone number
    - E mail address
  * Help desk
    - Telephone number
    - E mail address

- Location of important system documentation.
  * Login passwords
  * Operating system manuals
  * Software manuals

- Location of stored back up data.
  * For a system recovery.

- Location of hardware system documentation.
  * For local computer hosted server.

- Methods of access to local network configuration facilities.

- Methods of access to local hosted computer system.

Key Personnel

It is important to designate an individual or specific individuals to take responsibility of maintaining the computer server host and media server. These individuals should be properly vetted to ensure loyalty and adherence to the broadcast stations policies.

These individuals should have the following qualifications:

- Knowledge of computer system fundamentals.
- Knowledge of computer software fundamentals.

- Knowledge of networking fundamentals.
- Knowledge of Internet fundamentals.

- Knowledge of multimedia distribution fundamentals.

- Ability to configure and administer a local media server host computer.
- Ability to configure and administer a remote media server host computer.

- Ability to configure and administer all media server software.
- Ability to configure and administer all media server support software.

- Ability to configure and administer a network data uplink.

Physical

Physical security is the first line of defense against unauthorized access or use of a computer system. This prevents unauthorized people from gaining access to the computer system.

- Ensure that the computer hosting the media server is in a secure area.

- Ensure that access to the computer hosting the media server is limited to personnel that have a valid need.

- Ensure that the computer hosting the media server is connected to an uninterruptable power supply.
  * This will provide continuous service if the primary power provider fails.

- Ensure that the location of the media server is well ventilated and cooled.

- Ensure that the computer hosting the media server is connected to an alternate network provider.
  * This will provide continuous service if the primary network provider fails.

- Ensure that all electrical safety considerations are taken to prevent damage to the computer equipment.

- Log out of the computer hosting the media server when personnel are physically away from the computer system.

- Lock the computer screen when personnel are not directly in front of the computer system.

System

System security is the second line of defense against unauthorized access or use of a computer system. This will allow the computer to properly function as problems with the computer operating system are fixed with upgrades.

- Keep the operating system up to date.
  * It is extremely important to patch and update the computer system on a regular basis; especially critical updates.

- Do not install software that can allow unauthorized remote users to access the computer or allow malicious software to modify the computer system.

- THINK BEFORE YOU CLICK.

System security notifications

Official points of information for major operating systems:

Linux Redhat Security
access.redhat.com/security/updates

Linux Fedora Security
lists.fedoraproject.org/mailman/listinfo/security

Linux Debian Security
lists.debian.org/debian-security-announce/

Linux Ubuntu Security
www.ubuntu.com/usn

Linux Gentoo Security
www.gentoo.org/security/en/glsa/index.xml

OpenBSD Security
www.openbsd.org/security.html

FreeBSD Security
security.freebsd.org/

NetBSD Security
www.netbsd.org/support/security/advisory.html

Apple Security
ssl.apple.com/support/security/

Windows Security
technet.microsoft.com/en-us/security/bulletin

Fire Wall

Firewall security is the third line of defense against unauthorized access or use of a computer system. This application prevents unauthorized remote access to a computer using open data communications ports.

It is absolutely vital to properly configure the computer firewall. A poorly configured firewall is worse than having no firewall at all because it provides a feeling of false security.

If the media server is located on a remote network server, make sure that the following ports are open:
(Depending the services used.)

20 File Transfer Protocol (ftp) Data transfer
21 File Transfer Protocol (ftp) Control (command)

22 Secure Shell (SSH)

80 Hypertext Transfer Protocol (http)
443 Hypertext Transfer Protocol over SSL/TLS (https)

513 Remote Login (rlogin)
514 Remote Shell (rsh)
3389 Remote Desktop (rdesktop)

Designated port number for media server

NOTE:
If the Firewall has been activated without configuring the proper ports for remote access (ftp,ssh,rlogin,rsh or rdesktop) then the computer must be manually reconfigured at the remote location.

If the media server is located on a local network server, make sure that the following ports are open:
(Depending the services used.)

80 Hypertext Transfer Protocol (http)
443 Hypertext Transfer Protocol over SSL/TLS (https)

Designated port number for media server

A scan of the computer system hosting the media server should be conducted to verify which ports are open and closed. This can be accomplished with an online port scanner, and this will ensure that the firewall has been properly configured and is working correctly.

Software

Software security is the fourth line of defense against unauthorized access or use of a computer system. This will allow the media server software and media server support software to properly function as problems with the software are fixed with upgrades

- Make sure that the media server software is installed under the user account.

- Make sure that the media server support software is installed under the user account.

- Never install common operational software under the administrative or root account.

- Do not run common tasks as a root or administrative user.

- Make sure that the media server software is up to date.
  * Install patches and upgrades immediately upon notification.

- Make sure that all media server support software is up to date.
  * Install patches and upgrades immediately upon notification.

- Subscribe to the media server software's announcements list for security or maintenance issues.

- Subscribe to the media server support software's announcements list for security or maintenance issues.

- Periodically check the media server software's website for security or maintenance issues.

- Periodically check the media server support software's website for security or maintenance issues.

General software announcements:

United States Computer Emergency Readiness Team

Cyber Security Bulletins
www.us-cert.gov/current

Cyber Security Alerts
www.us-cert.gov/cas/techalerts/index.html

Cyber Security Bulletins
www.us-cert.gov/cas/bulletins

Password

Password security is the fifth line of defense against unauthorized access or use of a computer system. This is usually the weakest link in system security. The purpose of a password is to prevent unauthorized people from gaining access to a computer. Using simple or common words for passwords is the equivalent of not using any password protection.

- Select strong passwords for the ADMINISTRATOR / ROOT login. This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Select strong passwords for the USER login. This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Select strong passwords for the MEDIA SERVER software login. This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Do not use identical passwords for system logins.
  * Root – Different password
  * User – Different password
  * Media server – Different password

- Establish a set routine for changing ALL system passwords on a regular basis.
  * Root
  * User
  * Media server

- Do not store access passwords on the computer.

- Maintain physical security of all access password information.

File Transfer

Care should be used in the method of uploading data to a remote computer hosting the media server.

File Transfer Protocol (FTP) is a network protocol used to transfer files from one host to another host over a computer communications networks. This protocol does not use encrypted data transfer, which could allow the remote collection of sensitive login information or data.

There are alternatives for providing secure data transfer to remote computer systems.

Secure Shell (SSH) is a network protocol for secure data communication between two networked computers. This protocol allows remote shell services or command execution and other secure network services to be initiated using encryption.

Secure FTP (SFTP) is an application that uses SSH to transfer data files. It encrypts both commands and data unlike regular FTP. This prevents passwords and sensitive information from being transmitted in the clear over the network

FTP over SSH (not SFTP) is the practice of tunneling a normal FTP session through an SSH connection.

The following software applications can be used for secure file transfer:

OpenSSH

This is a FREE version of the SSH connectivity tool. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks. Additionally, OpenSSH provides secure tunneling capabilities and several authentication methods, and supports all SSH protocol versions.
www.openssh.com

PuTTY

This is a free and open source terminal emulator application which can act as a client for SSH, and remote login (rlogin). It can be used with the Windows and Unix operating systems.
www.chiark.greenend.org.uk/~sgtatham/putty

Remote Access - Command Line

The command line option of a remote computer system can be accessed to administer the hosted media server and computer system.

The following software applications can be used for remote access:

Remote login (rlogin) is a software utility for Unix-like computer operating systems that allows users to log in on a remote host via a computer communications network. The remote host must be running a rlogin daemon.

Remote shell (rsh) is a command line software utility that can execute user shell commands on a remotely networked computer. The remote system must be running the rsh daemon.

Neither rlogin or rsh provide encrypted data security. It is highly recommended that these applications are used with a Secure Shell (SSH) connection.

OpenSSH

This is a FREE version of the SSH connectivity tool. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks. Additionally, OpenSSH provides secure tunneling capabilities and several authentication methods, and supports all SSH protocol versions.
www.openssh.com

PuTTY

This is a free and open source terminal emulator application which can act as a client for SSH, and remote login (rlogin). It can be used with the Windows and Unix operating systems.
www.chiark.greenend.org.uk/~sgtatham/putty

Remote Access - Desktop

A graphical representation of a remote computer system desktop that can be accessed to administer the remotely hosted media server and computer system.

The following software applications can be used for remote access:

Remote Desktop Protocol (RDP) provides a user with a graphical interface of a remotely networked computer.
www.rdesktop.org

RDP does not provide encrypted data security. It is advisable to use this applications with a Secure Shell (SSH) connection.

OpenSSH is a FREE version of the SSH connectivity tool. OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other attacks. Additionally, OpenSSH provides secure tunneling capabilities and several authentication methods, and supports all SSH protocol versions.
www.openssh.com

System Logs

Monitoring the host computer and media server system logs can provide an immediate indication of system or software's breach, fault or trouble.

Monitor the host computer system logs for the following indications:

- Unusual activity

- Hardware fault

- Software fault

Monitor the media server logs for the following indications:

- Unusual activity

- Software fault

- Network fault

Data Management

This provides the ability to restore system operation if the integrity of the hardware or software has failed.

- Back up all host computer system files on a routine basis.
- Back up all media server software files on a routine basis.
- Back up all media server support software files on a routine basis.
- Keep all important documentation readily available.
- Keep all login information secure.
- Store computer back up data on removable media.
- Store software back up data on removable media.
- Store sensitive data on removable media.
- Store removable media in a secured area.
- Limit access to the stored removable media.

DOS / DDOS Attacks

A Denial Of Service attack (DoS attack) or Distributed Denial Of Service attack (DDoS attack) is an attempt to make a computer resource unavailable. The primary method of attack involves saturating the target computer with external communications requests. This prevents the computer from responding to legitimate traffic, or responding so slowly that it is rendered effectively unavailable.

Available software to prevent DOS / DDOS Attacks:

modsecurity
This is a type of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall.
www.modsecurity.org

Stateful Packet Inspection Firewall
A Login/Intrusion Detection and security application for Linux servers. This is a type of Firewall that keeps track of the state of network connections traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall. Packets that do not match a known active connection will be rejected.
www.configserver.com/cp/csf.html

Apache HTTP server modules

mod_evasive
This is designed to prevent HTTP DoS or DDoS attack or brute force attacks.

mod_bandwidth
This is a designed to limit per connection bandwidth use.

mod_ipconnlimit
This is a designed to limit simultaneous connections from the same IP address.